Strategic Culture Foundation

December 10, 2025 | EDITOR'S CHOICE

The former Israeli spies overseeing U.S. government cyber security

By Nate BEAR

Join us on Telegram, Twitter, and VK.

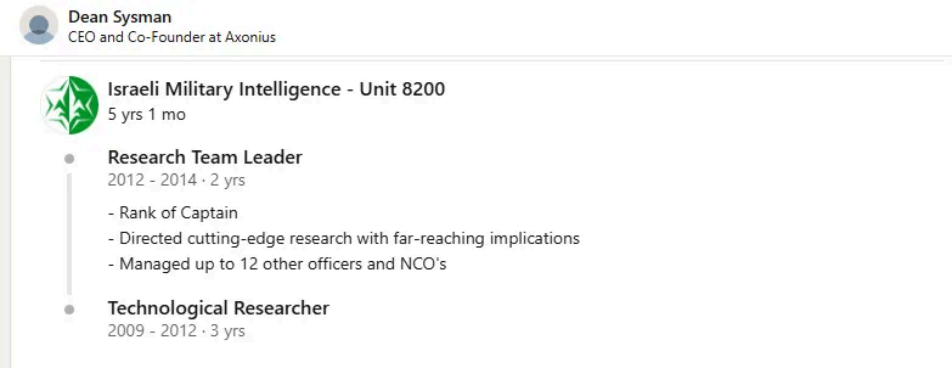
Contact us: info@strategic-culture.su

A company with deep ties to Israeli intelligence oversees cyber security across more than seventy US government agencies, including the Department of Defense and Homeland Security.

Axonius was founded by former spies in Israel's Unit 8200 and its software, which allows an operator 'visibility and control over all types and number of devices,' collects and analyses the digital data of millions of US federal employees.

The stated aim of the Axonius platform is to centralise IT tools to identity and fix security breaches. As a product of Israeli intelligence, however, the scale of Axonius's use across the US government raises serious questions.

Axonius was founded and is currently run by Israelis Dean Sysman, Ofri Shur and Avidor Bartov, who met in the 2010s while working on the same team within Israel's Unit 8200 spy service. On his LinkedIn profile, Sysman offers few details of their work for the IDF, describing it simply as having 'far-reaching implications.'



Sysman left the IDF in 2014 after five years and set up a cyber hacking outfit, while Shur and Bartov stayed on until 2017, a period which encompassed Israel's 2014 war of aggression against Gaza, during which the IDF murdered more than two thousand Palestinian civilians.

Axonius was established with curious speed. After leaving the IDF in 2017, Shur and Bartov teamed back up with Sysman and immediately received $4 million in seed funding from Yoav Leitersdorf, a San Francisco-based Israeli-American and fellow Unit 8200 veteran, to start Axonius. Leitersdorf, the managing partner at US-Israeli venture capital firm YL Ventures, is a prolific early-stage investor in Unit 8200 cyber start-ups.

The same year Sysman, Shur and Bartov also received millions in seed financing from Israeli firm Vertex Ventures which is run by veterans of Israel's spy units. Tami Bronner, a partner at Vertex, spent four years in Israeli military intelligence.

Following this early financing from investors close to Israel's intelligence establishment, the company went on to receive hundreds of millions in investment from a network of US venture capital firms with intelligence links to Israel.

These include Palo Alto-based Accel Partners, which has invested in more than thirty Israeli tech companies, including another Unit 8200 cyber spin-out, Oasis. Nir Blumberger, an Israeli who served in the IDF, was recruited by Accel from Facebook to open its Tel Aviv office in 2016.

Other Axonius backers include San Francisco-headquartered Bessemer Venture Partners which employs former Israeli intelligence operatives in a Tel Aviv office led by Adam Fisher. An American who emigrated to Israel in 1998, Fisher has acted as an intermediary between Zionists in Silicon Valley and the IDF, and during the genocide gave a presentation on how Israel can win the online war. Israeli Amit Karp, a partner at Bessemer Ventures and another former Israeli intelligence officer, sits on the Axonius board.

Menlo Park-based Lightspeed Venture Partners, which has backed Axonius with around $200 million over numerous funding rounds, also has significant ties to Israeli spy units. Yonit Wiseman, a partner at Lightspeed, spent six years in Israeli military intelligence, leaving in 2018. Her colleague, Tal Morgenstern, was a special forces commander in the IDF.

Given the evidence that Axonius is an Israeli intelligence cut-out, the scale of its penetration within the US federal government structure is extraordinary.

The company says its platform is 'deployed in more than 70 federal organizations' and is used by four of the five major US Department of Defense service agencies. The US federal government contract award website shows Axonius awards for the Army, Navy, Air Force and Marine Corps, which in itself means millions of personnel and their devices.

In November 2024, the company was selected by the Department of Homeland Security to modernise its cybersecurity abilities by centralising 'data coming from hundreds of separate data sources residing across dozens of federal, civilian, and executive branch agencies.' Just a month later, in December 2024, the company was contracted by the Department of Defense to upgrade its system of 24/7 surveillance which oversees all on-site and off-site DoD computers and IT networks, a capability known as 'continuous monitoring and risk scoring.' And in April this year Axonius obtained authorisation for any US federal agency to use its cloud-based cyber surveillance system.

Other federal departments integrating Axonius software include energy, transportation, the US Treasury and many others. Data from the US spending awards site shows the US Defence Logistics Agency, responsible for managing America's global weapons supply chain, is the single largest Axonius customer, spending $4.3 million in 2023 alone. The Department of Agriculture has paid nearly $2 million for Axonius tools and the Department of Health and Human Services has spent $1.3 million since 2021.

Axonius is commonly described as an American company. While its headquarters and administrative functions are in New York, its founders, senior executives, and its primary financiers are all Israeli, and, critically, its software and engineering functions are based in Tel Aviv. Axonius has more than eight-hundred employees, and a search of LinkedIn profiles confirms that a majority of Axonius's engineers in Tel Aviv have a background in Israeli military intelligence.

The pitch for the Axonius system is that it centralises data from all the security and IT tools an organisation uses into one place for easier analysis, control and fixes. And that place is Tel Aviv, where the hundreds of former Israeli spies working as engineers for Axonius have unprecedented access and visibility into the habits and movements of millions of US federal government employees.

With this visibility an Axonius operator can connect individual devices with individual IDs as well as seeing all login/logoff data and website usage. An operator can also order an account to be disabled, a device to be quarantined, or a user to be removed from a group.

In addition to this, Axonius has a separate R&D division within the company known as AxoniusX, a skunkworks unit focused on developing new cyber tools, run by another Unit 8200 spook, Amit Ofer.

Perhaps none of this matters, and Axonius is simply indicative of the sleazy, symbiotic nature of the relationship between the US and its colonial outpost.

This would be a fair argument if it wasn't for Israel's long history of espionage in the United States. From recruiting Hollywood producers who ran front companies that stole nuclear technologies, to selling bugged software to foreign governments, spying (especially cyber spying), has been central to Israel's foreign policy. Robert Maxwell, the father of Ghislaine Maxwell, was a spy for Israel, and a significant amount of circumstantial evidence suggests Jeffrey Epstein was also an Israeli military intelligence asset. More recently, during Trump's first term, Israel planted miniature spying devices around the White House and other US government buildings in Washington DC to monitor US officials.

US authorities, then, have allowed former spies from a country with a known history of espionage within the United States to establish a framework of cyber intelligence access across almost the entire federal government apparatus.

To put it another way, the US has effectively subcontracted its federal-level cyber security infrastructure to Israeli intelligence.

Whether Axonius has used, or has any intent to use its unprecedented access maliciously, is impossible to know. For anyone with knowledge of Israel's history of spying, however, the embedding of cyber software made by former Israeli spies within the US federal computer system network should raise serious alarms.

More broadly, Axonius shows how a militarised Israeli state takes billions in American funding every year to build its digital architecture of apartheid and genocide, and then sells these capabilities back to the US. American taxpayers, then, effectively pay Israel twice. And when the US buys back the technologies their taxpayers funded in the first place, they are inviting in trojan horse capabilities and making Israeli war criminals rich in the process.

The good news is that millions of ordinary Americans are wising up to the reality that Israel is not the great deal for the US that political leaders have, for so long, sold it as.

The Axonius story confirms, once again, just how bad this deal is.

Original article: **www.donotpanic.news**

© 2010 - 2025 | Strategic Culture Foundation | Republishing is welcomed www.strategic-culture.su.
The views of individual contributors do not necessarily represent those of the Strategic Culture Foundation.